

Client Alert

Current Issues Relevant to Our Clients

September 17, 2015

SEC Announces Areas of Focus for 2015 Cybersecurity Examinations

The Securities and Exchange Commission's ("SEC") Office of Compliance Inspections and Examinations recently issued a Risk Alert providing information on the areas of focus for the SEC staff's second round of cybersecurity examinations of registered investment advisers and broker-dealers. The examinations will focus on key topics including governance and risk assessment, access rights and controls, data loss prevention, vendor management, training and incident response. To assist firms in assessing their cybersecurity preparedness, the SEC staff included a sample document request in the Risk Alert. The entire Risk Alert is available [here](#).

Background

In 2014, the SEC staff conducted a series of examinations to identify cybersecurity risks and assess cybersecurity preparedness in the securities industry. Following those examinations, the SEC staff published guidance for registered investment advisers and registered investment companies related to cybersecurity preparedness in their business practices. For more information on the SEC staff's guidance see our Client Alert available [here](#). Given the continued importance of cybersecurity, the SEC staff announced a focus on cybersecurity compliance and controls as part of its 2015 Examination Priorities for investment advisers and broker-dealers. The Risk Alert provides additional information on the areas of focus for the SEC cybersecurity examinations, which will involve more testing to assess implementation of firms' procedures and controls.

What Will the Examinations Focus on?

The SEC's 2015 cybersecurity examination initiative is designed to build on previous examinations in this area. The initiative will further assess cybersecurity preparedness in the securities industry, including firms' ability to protect broker-dealer customer and investment adviser client information. Examiners will gather information on cybersecurity-related controls and will also test the implementation of certain firm controls. The initiative will focus on the following areas:

- **Governance and Risk Assessment:** Examiners may assess whether firms have cybersecurity governance and risk assessment processes relative to the areas of focus discussed below.

- **Access Rights and Controls:** Examiners may review how firms control access to various systems and data via management of user credentials, authentication and authorization methods. This may include a review of controls associated with remote access, customer logins, passwords, firm protocols to address customer login problems, network segmentation and tiered access.
- **Data Loss Prevention:** Examiners may assess how firms monitor the volume of content transferred outside of the firm by its employees or through third parties, such as by email attachments or uploads.
- **Vendor Management:** Examiners may assess how vendor relationships are considered as part of the firm's ongoing risk assessment process as well as how the firm determines the appropriate level of due diligence to conduct on a vendor.
- **Training:** Examiners may assess firms on whether the firm's training procedures are designed to encourage employees' understanding of and adherence to firm protocols with respect to technology.
- **Incident Response:** Examiners may assess whether firms have established policies, assigned roles, assessed system vulnerabilities and developed plans to address cybersecurity attacks and potential future breaches. This includes determining which firm data, assets and services warrant the most protection to help prevent attacks from causing significant harm.

While the primary focus for the SEC staff's exams are discussed above, examiners may select additional areas based on risks identified during the course of the examinations.

What Information Will Be Required in an Examination?

The Risk Alert also includes a sample request for information and documents regarding cybersecurity matters. The sample request includes, among other documents and information, requests for:

- policies and procedures related to the focus areas described above,
- information regarding the firm's periodic assessments of cybersecurity risks,
- information regarding the systems or applications used to authenticate access to secure information,
- information and agreements with third party vendors regarding cybersecurity,
- information regarding cybersecurity training programs including written training materials and
- information regarding the firm's processes for conducting tests or exercises of its incident response plans.

What Should Firms Do Now?

The Risk Alert is intended to encourage registered broker-dealers and investment advisers to reflect upon their own practices, policies and procedures with respect to cybersecurity. Firms should consider the SEC's key focus areas when reviewing their own practices, policies and procedures. Where the firm notices deficiencies, adjustments should be made to ensure compliance with the applicable guidance. Firms should also ensure all documents and information described in the Risk Alert are maintained properly and in an organized manner to facilitate document requests in future exams.

For More Information

To discuss any topic covered in this Client Alert, please contact a member of the Investment Management Group or visit us online at chapman.com.

This document has been prepared by Chapman and Cutler LLP attorneys for informational purposes only. It is general in nature and based on authorities that are subject to change. It is not intended as legal advice. Accordingly, readers should consult with, and seek the advice of, their own counsel with respect to any individual situation that involves the material contained in this document, the application of such material to their specific circumstances, or any questions relating to their own affairs that may be raised by such material.

To the extent that any part of this summary is interpreted to provide tax advice, (i) no taxpayer may rely upon this summary for the purposes of avoiding penalties, (ii) this summary may be interpreted for tax purposes as being prepared in connection with the promotion of the transactions described, and (iii) taxpayers should consult independent tax advisors.

© 2015 Chapman and Cutler LLP. All rights reserved.

Attorney Advertising Material.